



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,305	05/26/2000	STEFAN PHILIPP	PHD99-099	3907

7590 12/03/2003

Philips Electronic North American Corp.
580 White Plains Rd.
Tarrytown, NY 10591

EXAMINER

ARANI, TAGHI T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 12/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/555,305

Applicant(s)

PHILIPP, STEFAN

Examiner

Taghi T. Arani

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 May 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
- a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

Art Unit: 2131

DETAILED ACTION

Claims 1-14 were pending for examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yuliang Zheng, The SPEED Cipher, appeared in Financial Cryptography-First International Conference FC'97", February 1997 and further in view of Sprunk, US Pat. No. 5,404,402, issued April 1995.

As per claim 1, Zheng teaches the SPEED Cipher built on highly nonlinear Boolean functions, see Page 71, wherein, given a key K of l bits, SPEED scrambles a Plaintext M of w bits into a ciphertext of C of the same length see page 71.

Zheng teaches a block cipher method (i.e. The SPEED Cipher $f_i(x_1, k_i)$) where a cryptographic sub-operation is performed on Plaintext M internally represented as 8 words (x_0, x_2, \dots, x_7), each with w/8 bits, and a cryptographic key K expanded by the key scheduling function into four sub-keys k_1, k_2, k_3 and k_4 each K_i consists of r/4 words or round keys indicating the number of round in each pass. Zheng's sub-operations operate employing a different sub-key, as well as a different bit-wise operation on the plaintext X_i , see Figures 1 and 2 pages 72-73.

Zheng's fails to teach a bit-wise operation depending on a control function r_i based on random number.

Art Unit: 2131

However, Sprunk is directed to a secure microprocessor with reduced vulnerability to attack, see abstract.

In a preferred embodiment, Sprunk discloses a variable frequency source ("clock") which produces a clock signal with periodic clock pulses. That is, the variable selection of the microprocessor clock is affected using a random "modulation" circuit that randomly varies each pulse of the clock signal to render the timing of successive pulses unpredictable and used to clock a crypto processor for the encryption or decryption of data entered, see col. 3, line 66 through col. 4, line 13.

It would have been obvious to one of ordinary skill in the art to adapt the crypto processor implementing the SPEED Cipher of Zheng to that of Sprunk to prevent pirates to modify the operations of the crypto processor because the ability of pirates to observe such clock signals is critical in mounting a successful attack to the system security, see col. 1, lines 38-49.

As per claim 2, Zheng teaches one or more XOR (exclusive Or) combinations formed during the cryptographic sub-operations, see Page 74, table 2.

As per claim 3, Zheng teaches that data contain cryptographic keys (i.e. sub-keys) and /or operand (i.e. Xi plaintext), see Fig. 1 and Table 2.

As per claims 4-7, Zheng's SPEED Cipher uses the intermediate results from each round (sub-operation) as an operand for the subsequent Cryptographic sub-operations, see Fig.4, and that output of one round is fed ad an input to the succeeding round of operations, see Fig.2.

Zheng further teaches that during bit-wise operation seven 8-bit operand (xi) are invereted, see page 74, table 2.

Art Unit: 2131

Zheng further teaches that the bit values of a data bit word of plaintext or subkeys are inverted by means of an XOR operation, see, page 74, Table 2, For example in $P1 F1(x6, x5, \dots, x0) = x6x3 \text{ XOR } x5x1 \text{ XOR } \dots \text{ XOR } x0$ where $XiXj$ is bit-wise AND and $Xi \text{ XOR } Xj$ is the Bit-wise XOR of the two words and that in a pass Pi in SPEED the content in registers are updated accordingly, see page 76., see also the "Round transform" on page 78.

Claims 8-14 are apparatus claims corresponding to method claims 1-7, Claims 8-14 are rejected for the same reasons stated in the statement of rejection of claims 1-7 above.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner

November 24, 2003


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100